

Figure 1

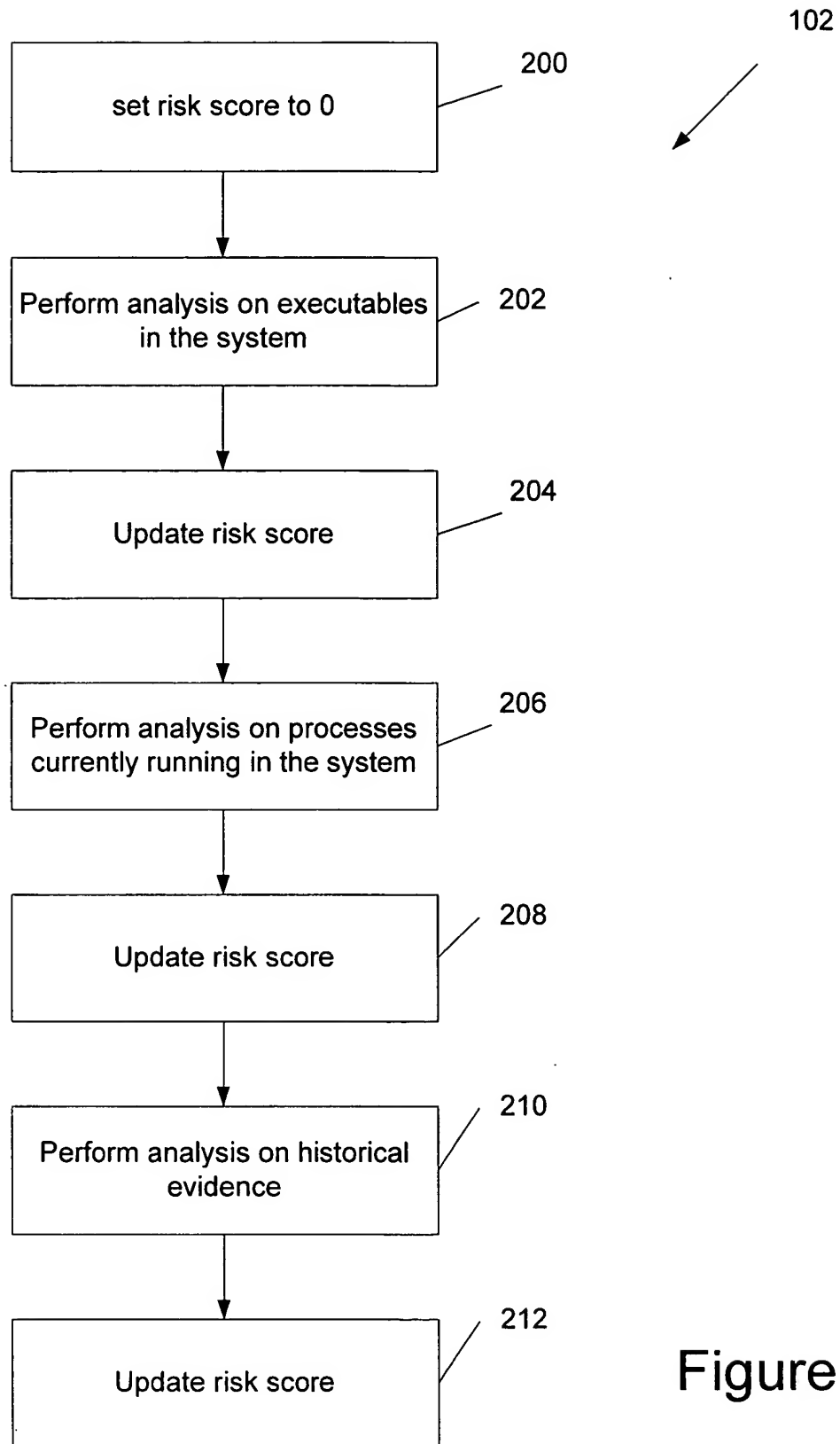


Figure 2

Subcategories	Criteria used to analyze executables	Risk value
Configuration	runs as a service	1
	runs under highly privileged account	1
	is not installed via a standard procedure	2
	has insufficient access control	1
	is recent	1
	is not signed	1
	modified date is not the same as created date	1
Capabilities	has networking capability	2
	has privilege manipulation capabilities	1
	has remote process capabilities	1
	can launch other processes	1
Misc. properties	has secure coding violations	1

Figure 3

Subcategories	Criteria used to analyze running processes	Risk value
Configuration	has higher effective privilege	1
	has more privileges than the process should have	1
	has loaded in extra dynamic libraries	1
Capabilities	owns system objects that do not have sufficient access control	1
	owns UDP port (sending)	1.5
	owns UDP port (listening)	2
	owns TCP port (sending)	0.5
	owns TCP port (listening)	1

Figure 4

Run-time analysis criteria	Risk value
launches child processes without complete path specification	1
launches child processes that inherit privileges	1
exhibits different attributes/behavior given different arguments	1
impersonates users	1

Figure 5